Mobile Access to Port and Maritime Data

Daniel Elroi
NorthSouth GIS LLC

AAPA Security & IT Conference
Arlington, VA, July 21, 2016
The GIS Experts in Ports

Company
- Founded in 2005
- Headquarters in Los Angeles
- An integral member of the Ports industry Ecosystem

- Esri Gold Partner since 2010, Esri's leading partner in ports
- Genetec, PureActiv, AssetWorks, Maintstar, Lenel, NICE, Milestone
- Esri, Latitude Geographics, Mariner Group, ROK Technologies
NSG US Ports 2008 - 2016

- Los Angeles – 2008
- Stockton – 2011
- Oakland – 2012
- Tacoma – 2013
- Tampa - 2014
- Long Beach – 2014
- Hueneme – 2015
- San Diego – 2015
- Houston – 2016
- Charleston – 2016
200+ Tasks, 50,000+ Hours in Ports to Date
Mobile Access to Data
Ports Want Their Data Like This
Instead of Like This
So That When These Things Happen
They Can Do This
Instead of This

Photo credit: Nanette Stark, Washington Department of Fish and Wildlife
This Means…

Mobile Access
But… But… But…

- Security sensitive information
- Cybersecurity
- Infrastructure
- Data plans
- Network traffic
- Firewalls
- Identity management
- Policies
- Distractions
Once Again…

Photo credit: Nanette Stark, Washington Department of Fish and Wildlife
Case Studies

- Los Angeles
- Stockton
- Oakland
- Tacoma
- Tampa
- Long Beach
- Hueneme
- San Diego
- Houston
- Charleston
Case Studies

- Los Angeles
- Stockton
- Oakland
- Tacoma
- Long Beach
- Hueneme
- San Diego
- Houston
- Tampa
- Charleston
Port of Stockton

- Catalysts for GIS
  - Security
  - Property Management
- Stance towards cloud
  - Very cautious
GIS Architecture

- Esri-based Enterprise GIS infrastructure
- NSG Port Solution implementation
- Widely-used GIS map viewer (*geoPORTal*)
- Integration of GIS with:
  - USCG AIS
  - Mariner’s CommandBridge
  - Saab’s KleinPort
  - Radio and sign alerting systems
  - HipLink mass notification
Approach 1: Wireless WAN

• Wireless mesh network for Port Police use

• Users are part of the security LAN, so all network security is internal to port

• Access CommandBridge and GIS from cars

• Transmit in-dash cameras to office and other cars
Approach 2: Public Internet, Internal Security

- Public internet via cellular data for non-security users
- Reverse proxy to isolate internal resources
- Active Directory for identity management
- Tablet access to GIS in field
- Asset inspections contained to LAN
- Real time updates from field
Port of Oakland

- Catalysts for GIS
  - Security
  - Engineering
- Stance towards cloud
  - Cautious
GIS Architecture

- Esri-based Enterprise GIS infrastructure
- NSG Port Solution implementation
- Widely-used GIS map viewer (PortView)
- Integration of GIS with:
  - Marine Exchange AIS
  - SendWordNow Mass Notification
  - Genetec Video Management System
- Special modules
  - Incident reporting and management
  - Asset inspection
Approach: Build Resiliency, Buffer the Risk

- Primary GIS internal
- Replicated data and web GIS sites in private cloud
- All external access, incl. data capture uses cloud site
- Very narrow controlled pipe to the outside
Port of Tacoma / Northwest Seaport Alliance

- Catalysts for GIS
  - Security
  - Property Management
  - Asset Management
- Stance towards cloud
  - Careful but open
GIS Architecture

- Esri-based Enterprise GIS infrastructure
- NSG Port Solution implementation
- Widely-used GIS map viewer (PortView)
- Integration of GIS with:
  - Marine Exchange AIS
  - PureActiv Video Management System
- Possible future integrations
  - Yardi lease management
  - Maximo
Approach 1: Public Network, Private LAN

- Public Safety internet access
- VPN into intranet
- Authentication on LAN
- Access to GIS viewers, cameras from police cars
Approach 2: Use Public Cloud to Map Assets

- Place copies of port data in secure location on Esri’s public cloud
- Share information with contractors, field crews
- Use SaaS software to verify/update data
- Reduce/eliminate impact on IT
- Eliminate exposure of IT LANs
- High security
- Low cost
Recap

• No cloud – Private cloud – Public cloud
• Intranet – Extranet – Internet
• LANs – Extended LANs – VPN LANs
What are your thoughts?